IN THE UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF OHIO WESTERN DIVISION AT CINCINNATI

FINESSE EXPRESS, LLC, individually and on behalf of all others similarly situated,
1880 Braselton Highway, Suite 118 #5065
Lawrenceville, GA 30043

AND

WIDER GROUP, INC., individually and on behalf of all others similarly situated,
333 N. Alabama St., Suite 350
Indianapolis, IN 46204

Plaintiffs,

v.

TOTAL QUALITY LOGISTICS, LLC,
% Brent Willis, Registered Agent
4017 Washington Avenue
Lorain, OH 44052

Defendant.

Case No. 20-cv-235

Judge

Magistrate Judge

CLASS ACTION COMPLAINT FOR DAMAGES

JURY TRIAL DEMANDED

Plaintiffs Finesse Express, LLC ("Finesse") and Wider Group, Inc. ("Wider") (collectively the "Plaintiffs"), individually and on behalf of all other similarly situated persons, by and through their undersigned attorneys, files this Class Action Complaint against Total Quality Logistics, LLC ("TQL" or "Defendant"), and alleges the following based on personal knowledge, the investigation of counsel, and information and belief:

NATURE OF THE ACTION

1. With this action, Plaintiffs seek to hold TQL responsible for the harm it caused them and the tens of thousands of similarly situated persons in the massive (and preventable) data breach TQL announced in February 2020.

2. TQL is the second largest freight brokerage firm in North America, providing freight transportation and logistics services to customers across the country and internationally. As a broker, TQL contracts with motor carriers to pick up and deliver the freight of its customers to transport loads to their necessary destinations.

3. Plaintiffs and the other members of the Class (as defined below) are motor carriers and freight customers who contracted with TQL to connect them with freight loads needing delivered locally, regionally, and nationally.

4. To do business with TQL, Plaintiffs and the Class were required to provide TQL with certain personal and financial information under the understanding that TQL would keep this information confidential and secure. Plaintiffs and the Class trusted TQL to protect their personal and financial information. Yet this trust was misplaced.

5. On or around February 27, 2020, Defendant announced that hackers had infiltrated its information technology ("IT") systems earlier that month and had gained unauthorized access to the Sensitive Information of Plaintiffs and the Class, including "tax ID numbers, bank account numbers, and invoice information, including amounts and dates"[1] (the "Data Breach" or "Breach").

[1]Clarissa Hawes, "Breaking News: Carriers Notified of Hacker Data Breach of TQL's IT Systems," FREIGHT WAVES (Feb. 27, 2020), https://www.freightwaves.com/news/breaking-carriers-notified-of-hacker-data-breach-of-tqls-it-systems (quoting email sent to carriers by Kerry Bryne, president of TQL, on February 23, 2020).

6. As a result of Defendant's reckless and wanton failure to implement adequate IT security measures that reasonably conformed with industry standards, hackers have now accessed, viewed, and, in a growing number of cases, used the private and confidential financial information, including tax ID numbers, bank account numbers, Social Security numbers, invoice information, and other highly confidential information (collectively, the "Confidential Information") of Plaintiffs and the Class.

7. This class action seeks to redress TQL's many failures that caused cyber criminals and identity thieves to access Plaintiffs' and the Class's Confidential Information. Because of the Breach, Plaintiffs have suffered damages and all members of the Class are at imminent risk of serious and crippling identity theft, which, as TQL has admitted, has already begun to occur to Plaintiff Finesse and other members of the Class.[2]

8. The increased risk of fraud and identity theft is alone a significant injury to Plaintiffs and the Class, as it places each of these small businesses and sole proprietors in the position of having to divert company resources away from transporting freight during a urgent time of nationwide supply-chain crisis,[3] and instead expend company resources monitoring accounts and interfacing with the understaffed IRS to prevent business identity theft and the potentially bankruptcy-inducing problems that could result. Plaintiff Finesse and other Class

[2]"Notice of Carrier Data Breach," TQL (Updated: 5:33 p.m. EST Feb. 28, 2020), https://www.tql.com/carrierhotline (stating that nearly twenty carriers have been identified as already experiencing "ACH payment theft").

[3]*See, e.g.*, Aarian Marshall, *As COVID-19 Spreads, Truckers Need to Keep Trucking*, WIRED (Mar. 20, 2020), https://www.wired.com/story/covid-19-spreads-truckers-keep-trucking/ (describing the urgent need for truckers to move necessary supplies, including medical equipment and cleaning supplies). On March 18, 2020, the Federal Motor Carrier Safety Administration ("FMCSA") expanded a previously declared Emergency Declaration under 49 C.F.R. § 390.23, exempting drivers from the Hours of Service regulations based on the urgent need for the transportation of essential supplies, equipment, and persons needed to respond to the national emergency created by the COVID-19 outbreak. *See* Expanded Emergency Declaration Under 49 C.F.R. § 390.23, No. 2020-002, DEP'T OF COMMERCE: FMCSA (Mar. 18, 2020), https://www.fmcsa.dot.gov/sites/fmcsa.dot.gov/files/2020-03/EXPANDED%20EMERGENCY%20DECLARATION%20UNDER%2049%20CFR%20%C2%A7%20390.23%20No.%202020-002.pdf.

members have already experienced fraudulent transactions and all members will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost business opportunities, paid and unpaid overtime, lost time and expenses mitigating harms, increased risk of harm, diminished value of the Confidential Information, loss of privacy, and/or additional damages as described below.

9. Accordingly, Plaintiffs bring this action individually and on behalf of the Class, seeking compensatory and punitive damages, restitution, and injunctive and declaratory relief, along with the reasonable attorney fees, costs, and expenses incurred in bringing this action.

THE PARTIES

10. Plaintiff Finesse Express, LLC is a Georgia limited liability company and a citizen of Georgia. Finesse is a motor carrier with one truck that has contracted with TQL for freight brokerage services.

11. Plaintiff Wider Group, Inc. is an Indiana corporation with its principal place of business in Indianapolis, Indiana. Wider is a motor carrier with 150 trucks that has contracted with TQL for freight brokerage services.

12. Defendant Total Quality Logistics, LLC is an Ohio limited liability company and a citizen of Ohio, with its principal place of business located at 4289 Ivy Pointe Boulevard, Cincinnati, OH 45245.

JURISDICTION AND VENUE

13. This Court has diversity jurisdiction over this action under the Class Action Fairness Act (CAFA), 28 U.S.C. § 1332(d), because this is a class action involving more than

100 class members, the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and at least one member of the class is a citizen of a state different from Defendant.

14. This Court has personal jurisdiction over Defendant because it is a citizen of this state and its principal place of business is in this State. Venue is likewise proper as to Defendant in this District because "a substantial part of the events or omissions giving rise to the claim occurred in this District." 28 U.S.C. § 1391(b)(2).

FACTUAL ALLEGATIONS

15. Plaintiffs incorporate by reference all allegations of the paragraphs 1–9 as though fully alleged here.

A. Anatomy of a Data Breach

16. On February 27, 2020, TQL sent a mass email to its carriers and customers informing them that their information may have been compromised in a data breach of TQL's IT systems that the company had discovered on February 24, 2020.

17. The email that Plaintiff Finesse received, attached as Exhibit A, stated the following:

> We wanted to make you aware that we have uncovered a breach of our IT systems. This breach compromised the security of our online portals for many of our carriers. We believe that external hackers gained access to your tax ID number, bank account numbers, and invoice information, including amounts and dates.

18. Plaintiff Wider received the same email.

19. The email acknowledged that this would cause inconvenience to affected customers and carriers and that financial harm would likely occur, stating:

> We sincerely apologize for the inconvenience and concern we know this causes you. We would recommend that you contact your financial institution immediately, letting them know your bank information has been exposed. They

> will be able to advise you on the best next steps to further protect you and your information.

If you have additional concerns, you can visit FTC's website at IdentityTheft.gov.

20. Despite acknowledging the inconvenience and high risk of fraud the Data Breach created for Plaintiffs and the Class, Defendant failed to offer any sort of compensation or reimbursement for the significant expenses its carriers would incur because of this Breach.

21. Instead, TQL attempted to shift all of the costs for its failure to safeguard the Confidential Information onto the victims of its negligence—Plaintiffs and the Class.

22. Trucking industry blogs have uncovered additional information about the Breach that TQL has yet to publicly acknowledge. In an article published February 28, 2020, Freight Broker Live reported the following:

> According to internal sources, the breach was discovered earlier in the week when TQL's accounting department called a carrier to verify changes to their banking information within their system. The carrier reportedly denied knowledge of the change prompting the accounting department to send the issue to the IT department within TQL. Sources say there is evidence the breach occurred *quite a while before being discovered*, although it is unclear of [sic] just how long the hackers were dormant in the system. It appears several carrier's [sic] banking information was changed and that payments were sent out to these altered bank accounts. Internal sources say the total amount stolen was less than $100,000. TQL says they have identified less than 20 carriers where ACH payment theft may have occurred.[4]

23. Of course, since hackers accessed the tax ID numbers, bank account numbers, and invoice data of many thousands of carriers and customers, the amount of money stolen as a result of this Breach is only going to rise.

[4]Stephen Oatley, *TQL Data Breach Update: What We Know*, FREIGHT BROKER LIVE (Feb. 28, 2020), http://www.freightbrokerlive.com/tql-data-breach-update-what-we-know/ (emphasis added).

24. In fact, Plaintiff Finesse has identified unauthorized fraudulent charges as recently as March 16, 2020. He is also taking time away from driving and finding loads to police his ban accounts and communicate with his bank to correct these fraudulent charges.

25. While TQL has attempted to closely control all information on the possible causes of the Breach, some information has leaked out. Freight Broker Live uncovered one possible cause of the Breach:

> Sources tell Freight Broker Live the hackers were able to access the internal IT systems utilizing TQL's mobile applications as a pass through into the system. TQL has since taken steps to close the security gaps in their system, hired an [sic] third-party cyber security firm for "additional forensics," on their systems to identify if any other information was compromised. TQL is also working with the Federal Bureau of Investigation and other law enforcement to track the hackers.[5]

26. Another article quotes TQL CEO Terry Byrne as stating: "We are still gathering details, but it appears it was initially an information/data phishing attempt."[6]

27. One thing that TQL has tried to emphasize is that "the data breach was not a malware or ransomware attack."[7]

28. Through discovery, Plaintiffs and the Class will uncover the precise failures that caused the Data Breach. But whether the Breach occurred through errors in its mobile application, a lack of necessary email filtering and/or anti-phishing training, improperly segmented networks, or other failures, one thing is clear: the Breach should not have occurred.

---

[5] *Id.*
[6] Clarissa Hawes, *UPDATE: TQL Says Data Breach Was Not Malware or Ransomware Attack*, FREIGHTWAVES (Feb. 27, 2020), https://www.freightwaves.com/news/update-tql-says-data-breach-was-not-malware-or-ransomware-attack.
[7] *Id.*

29. Had TQL taken the well-known risk of cyber intrusion seriously and adequately tested, audited, and invested in its IT systems and adequately trained its staff to vigilantly detect vulnerabilities and intrusions, the Data Breach would never have occurred.

30. After all, data breaches are preventable.[8]

B. Cyber Criminals Have Used and Will Continue to Use Carriers' Confidential Information to Defraud Them

31. Personal and business information is of great value to hackers and cyber criminals, and the Confidential Information stolen in the Data Breach can and will be used in a variety of sordid ways for criminals to exploit Plaintiffs and the Class Members and to profit off their misfortune.

32. Each year, identity theft causes tens of billions of dollars of losses to victims in the United States.[9]

33. While people often think of individuals suffering from identity theft, business identity theft is just as, if not more, financially devastating.

34. A businesses tax ID number, also known as an employer identification number or EIN, is the equivalent of a business's Social Security number.

35. Business identity theft can occur, including the opening of fraudulent accounts, with just a business name, address, and EIN.[10]

---

[8] *See* Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012) (discussed *infra* ¶ 69).

[9] "Facts + Statistics: Identity Theft and Cybercrime," Insurance Info. Inst., https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime (discussing Javelin Strategy & Research's report "2018 Identity Fraud: Fraud Enters a New Era of Complexity").

[10] "Use of Business EINs for Tax Fraud," BusinessIDTheft.org, http://www.businessidtheft.org/Education/BusinessIDTheftScams/BusinessEINandTaxFraud/tabid/226/Default.aspx (last accessed Mar. 20, 2020).

36. On September 23, 2013, the Treasury Inspector General for Tax Administration (TIGTA) published an audit report entitled "Stolen and Falsely Obtained Employer Identification Numbers are Used to Report False Income and Withholding." TIGTA conducted the audit because "perpetrators of fraud are using stolen or falsely obtained EINs to submit tax returns with false income and withholding documents to the IRS for the sole purpose of receiving a fraudulent tax refund."[11]

37. The TIGTA audit found that "the IRS could issue almost $2.3 billion in potentially fraudulent tax refunds based on stolen or falsely obtained EINs each year, and roughly $11.4 billion over the next five years."[12]

38. These criminal activities would result in devastating financial and personal losses to Plaintiffs and the Class Members.

39. This was a financially motivated Breach, as the only reason the cyber criminals went through the trouble of infiltrating TQL's IT systems was to get the information that would enable them to engage in wire fraud, identity theft, tax fraud, and the innumerable other criminal activities the unscrupulous can engage in with access to a companies' most sensitive Confidential Information.

40. This is not just speculative. As the FTC has reported, if hackers get access to Confidential Information, they will use it.[13]

41. Hackers may not use the information right away. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

---

[11] *Id.*
[12] *Id.*
[13] Ari Lazarus, *How fast will identity thieves use stolen info?*, FED. TRADE COMM'N (May 24, 2017), https://www.consumer.ftc.gov/blog/2017/05/how-fast-will-identity-thieves-use-stolen-info.

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[14]

42. With this Data Breach, identity thieves have already started to prey on TQL carriers, and we can only anticipate that this will continue.

43. Victims of data breaches who have already suffered fraud, like Plaintiff Finesse and other Class Members, must spend countless hours and large amounts of money repairing the impact to their credit.[15]

44. And the fact that others have already suffered fraudulent transactions causes other victims, such as Plaintiff Wider to be all the more vigilant and spend more and more company time preparing for and protecting against an imminent risk of certainly impending fraud.

45. While some harm has begun already, the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs versus when it is discovered, and also between when Confidential Information is stolen and when it is used.

46. As a direct and proximate result of the Data Breach, Plaintiffs and the Class have suffered actual identity theft and/or have been placed at an imminent, immediate, and continuing increased risk of harm from continued fraud and identity theft. Plaintiffs and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, and closely

---

[14] *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO, July 5, 2007, https://www.gao.gov/assets/270/262904.htmlu (emphasis added).

[15] "Guide for Assisting Identity Theft Victims," Federal Trade Commission, 4 (Sept. 2013), http://www.consumer.ftc.gov/articles/pdf-0119-guide-assisting-id-theft-victims.pdf.

reviewing and monitoring bank accounts, and credit reports for unauthorized activity for years to come. Even more seriously is the identity restoration that Plaintiff Finesse and other Class Members must go through, spending countless hours filing police reports, filling out IRS forms, Federal Trade Commission checklists, Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

47. Plaintiffs and the Class have suffered, and continue to suffer, actual harms for which they are entitled to compensation, including:

a. Actual identity theft, including fraudulent transactions on bank accounts;

b. Trespass, damage to, and theft of their personal property including Confidential Information;

c. Improper disclosure of their Confidential Information;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their Confidential Information being placed in the hands of criminals and having been already misused;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cyber criminals have their Confidential Information and that identity thieves have already used that information to defraud Plaintiff and members of the Class;

f. Substantial opportunity costs, including lost profits and business opportunities, incurred from taking time away from driving and locating loads to respond to the Data Breach, including, among other things, policing bank accounts, disputing

fraudulent transactions, canceling and opening new bank accounts, and contacting the IRS to protect themselves from tax fraud;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the data breach;

h. Ascertainable losses in the form of deprivation of the value of the Confidential Information for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, and/or funds;

j. Damage to their credit due to fraudulent use of their Confidential Information; and

k. Increased cost of borrowing, insurance, deposits and other items which are adversely affected by a reduced credit score.

48. Moreover, Plaintiffs and Class have an interest in ensuring that their information, which remains in the possession of Defendant, is protected from further breaches by the implementation of security measures and safeguards.

49. Defendant itself acknowledged the harm caused by the Data Breach because it urged Plaintiffs and the Class to "immediately" contact their banks and follow their bank's advice "to further protect you and your information." *See* Exhibit A.

C. Defendant was Aware of the Risk of Cyber-Attacks and Could Have Prevented the Data Breach

50. Data security breaches have dominated the headlines for the last two decades, and it doesn't take an IT industry expert to know that major businesses like TQL are at risk.

51. The general public can tell you the names of some of the biggest data breaches: LabCorp, Quest Diagnostics, Yahoo, Equifax, Marriott International, Target, Home Depot, Anthem, Heartland Payment Systems, and TJX Companies, Inc.[16]

52. The Federal Trade Commission has interpreted Section 5 of the Federal Trade Commission Act of 1914 ("FTC Act"), 15 U.S.C. § 45, to classify a company's failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice. *See, e.g.*, *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 245-47 (3rd Cir. 2015); *In re BJ's Wholesale Club, Inc.*, 140 F.T.C. 465 (2005).

53. In 2007, the FTC published guidelines that establish reasonable data security practices for businesses. The guidelines note that businesses should protect the confidential information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems. The guidelines also recommended that businesses consider using an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.

54. The FTC has also published a document titled "Protecting Personal Information; A Guide for Business" that highlights the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[17]

---

[16]*See, e.g.*, Taylor Armerding, *The 18 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Dec. 20, 2018), https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html.

[17]FTC, *Protecting Personal Information: A Guide for Business*, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last accessed Mar. 20, 2020).

55. Upon information and belief, TQL failed to implement reasonable industry standards necessary to prevent a data breach, including the FTC's guidelines.

56. Likewise, TQL failed to create, maintain, and/or comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of personal information and reasonably conformed to an industry recognized cybersecurity framework.

57. Because of its failure to create, maintain, and/or comply with a necessary cybersecurity program, TQL was unable to ensure the protection of information security and confidentiality, protect against obvious and readily foreseeable threats to information security and confidentiality or the unauthorized access of the Confidential Information.

58. Not only did TQL comply with the FTC guidelines, it also failed to meet the minimum standards of any the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); the Center for Internet Security's Critical Security Controls (CIS CSC); or members of the ISO/IEC 27000 family.

59. As a massive, sophisticated, and immensely profitable company doing business in all 50 states and Canada, there is no excuse for TQL's failure to invest adequate financial and temporal resources into creating, maintaining, or complying with a minimally adequate cybersecurity program.

60. In requesting that Plaintiffs and the Class provide TQL with their most sensitive Confidential Information, TQL represented to Plaintiffs and the Class that it understood the importance of protecting their Confidential Information and that it would do so as a part of their

agreement. TQL represented to Plaintiffs and the Class through its confidentiality provision in its broker-carrier agreements, its stated privacy policies, and its company security practices that it maintained robust procedures designed to carefully protect the Confidential Information with which it was entrusted.

61. The broker-carrier agreement that TQL requires carriers to sign explicitly promises that TQL would protect the Confidential Information of Plaintiff and the Class and expressly provided a remedy for the failure to do so:

> **CONFIDENTIALITY**. In addition to confidential information protected by law, whether statutory or otherwise, the Parties agree that all of their financial information and that of CUSTOMERS, including, without limitation, freight and brokerage rates, amounts received for brokerage services, amounts of freight charges collected, amounts of freight charges paid, freight volume requirements, as well as related CUSTOMER information, CUSTOMER shipping or other logistic requirements shared or learned between the Parties and CUSTOMERS shall be treated as confidential, and shall not be disclosed or used for any reason without prior written consent by the Parties. If confidentiality is breached, the Parties agree that the remedy at law, including monetary damages, may be inadequate and that the Parties shall be entitled, in addition to any other remedy available, to an injunction restraining the violating Party from further violation of this Agreement.

See, e.g., **Exhibit B** (Broker-Carrier Agreement between TQL and Finesse Express, LLC, executed June 5, 2019, ¶ 21).

62. The Broker-Carrier Agreement that TQL uses is a form agreement that it makes all motor carriers sign in order to do business with it.

63. The Agreement attached as Exhibit B is substantially the same as that which Plaintiff Wider and all other Class members entered into with TQL.

64. The Agreement that TQL and Plaintiff Wider signed is incorporated by reference.

65. The Confidential Information exposed in the Data Breach falls under this provision.

66. TQL violated this provision by not treating the Confidential Information as confidential when it failed to implement the necessary data security policies, rules, and procedures to protect the Confidential Information from hackers.

67. As TQL agreed, monetary damages alone are not adequate to fully remedy its breach of the confidentiality agreement and thus Plaintiffs and the Class are entitled to an injunction ordering TQL to protect their Confidential Information, in addition to monetary damages.

68. It was possible for TQL to keep the Confidential Information of Plaintiffs and the Class confidential.

69. Data breaches are preventable.[18] As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[19] She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."[20]

70. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[21]

---

[18]Lucy L. Thomson, "Despite the Alarming Trends, Data Breaches Are Preventable," *in* DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012).
[19]*Id.* at 17.
[20]*Id.* at 28.
[21]*Id.*

71. In a Data Breach like this, many failures laid the groundwork for the success (from the cyber criminal's view) of the Breach.

72. For example, TQL's IT systems lacked the necessary encryption to maintain the confidentiality of the sensitive Confidential Information Plaintiff and the Class entrusted to TQL.

73. TQL also failed to properly segment its network, permitting intruders to move freely once in the IT system to find and extract the most valuable information.

74. TQL also failed to adequately test and audit its system, failed to adequately monitor its system for intrusions, and failed to create and enforce appropriate industry-standard security policies, rules, and procedures.

75. To the extent the Breach was caused by phishing attacks, these are readily preventable through industry standard email filtering software and regular awareness training for staff, and the harm from phishing-related breaches can be minimized through proper network segmentation and encryption of all confidential information.

76. Had TQL exercised reasonable care, the Data Breach would not have happened and Plaintiffs and the Class would not have suffered the injuries they are continuing to face.

D. Plaintiffs' Experiences

77. Plaintiff Finesse has suffered actual damages as a result of this Data Breach.

78. In the weeks following the February 27 email from TQL, Finesse has spent approximately 15 hours responding to the Data Breach, including reviewing every transaction that comes through its company bank accounts.

79. Finesse has identified three fraudulent transactions that occurred since late February, and it is having to spend company time away from driving and acquiring loads contesting these charges and on the phone with the fraud department at Finesse's bank.

80. Already because of the time that it has had to spend responding to the Breach, Finesse has missed out on business opportunities, including an 890 mile load worth around $2,500 that Finesse would have been able to acquire but for the time it had to spend responding to the Data Breach.

81. Plaintiff Wider has spent time responding to the Data Breach including time on the phone with its financial institution and time monitoring company bank accounts.

82. Plaintiff Wider is at increased risk of fraud and business identity theft because of the Breach and has already lost company time spent responding to the Data Breach.

83. Because bank account numbers and EINs were accessed by hackers in the Data Breach, both Plaintiffs will have to spend significantly more time responding to this Data Breach.

84. Plaintiffs agreed with TQL that TQL would keep their business and financial information confidential, and now because TQL has failed to do so, Plaintiffs are left holding the bag.

85. TQL should be held responsible for the damages it has caused Plaintiffs and the Class through the Data Breach.

CLASS ACTION ALLEGATIONS

86. Plaintiffs incorporate by reference the allegations from the preceding paragraphs as if fully restated here.

87. Plaintiffs bring this action against TQL individually and on behalf all others similarly situated under Federal Rule of Civil Procedure 23. Plaintiffs assert all claims on behalf of a nationwide Class defined as follows:

> **All persons whose sensitive personal and business information, including Social Security numbers or Tax ID numbers, bank account numbers, and was compromised as a result of the Data Breach at Total Quality Logistics, LLC announced in February 2020.**

88. Excluded from the Class are Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and judicial staff.

89. Plaintiffs reserve the right to amend the above definition or to propose other or additional subclasses in subsequent pleadings and motions for class certification.

a. Class Certification is Appropriate

90. The proposed Class and any additional subclasses meet the requirements of Fed. R. Civ. P. 23(a), (b)(1), (b)(2), (b)(3), and (c)(4).

91. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. Defendant has not publicly disclosed the total number of individuals affected, but based on publicly available information the Class appears to exceed 85,000 members.

92. **Typicality:** Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all members of the Class were injured through TQL's uniform misconduct. The same event and conduct that gave rise to Plaintiffs' claims are identical to those that give rise to the claims of every other Class member because Plaintiffs and each member of the Class had their Confidential Information compromised in the same way by the same conduct of TQL. Similarly,

all members of the Class entered into uniform contracts with TQL that contained substantially the same confidentiality agreement that TQL violated through its actions and inactions that caused the Data Breach.

93. **Adequacy:** Plaintiffs are adequate representatives of the Class because Plaintiffs' interests do not conflict with the interests of the class that they seeks to represent; Plaintiffs have retained counsel competent and highly experienced in data breach class action litigation; and Plaintiffs and Plaintiffs' counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiffs and their counsel.

94. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiffs and the Class. The injury suffered by each individual class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for members of the class individually to effectively redress TQL's wrongdoing. Even if class members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

95. **Commonality and Predominance:** There are many questions of law and fact common to the claims of Plaintiffs and the other members of the Class, and those questions

predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant failed to adequately safeguard Plaintiffs' and the Class's Confidential Information;

c. Whether Defendant owed a duty to Plaintiffs and the Class to adequately protect their Confidential Information, and whether it breached this duty;

d. Whether Defendant's conduct, including its failure to act, resulted in or was the proximate cause of the Breach of its company IT systems;

e. Whether Plaintiff and the Class were injured as a proximate and foreseeable result of Defendant's breach of its duties to Plaintiffs and the Class;

f. Whether Defendant had a contractual obligation to maintain the confidentiality of the Confidential Information of Plaintiffs and the Class, and whether Defendant breached that duty;

g. Whether Plaintiffs and the Class suffered damages as a result of Defendant's breach of its contractual duty to maintain the confidentiality of their Confidential Information;

h. Whether Defendant continues to breach duties to Plaintiffs and the Class;

i. Whether Plaintiffs and the Class suffered injury as a proximate result of Defendant's negligent actions or failures to act;

j. Whether Defendant was unjustly enriched by its failure to adequately invest in minimum data security measures necessary to protect the Confidential Information; and

k. Whether Plaintiffs and the Class are entitled to recover damages, restitution, declaratory, injunctive and other equitable relief, and attorney fees, costs, and expenses.

CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(On Behalf of the Class)

96. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

97. Defendant TQL solicited, gathered, and stored the Confidential Information of Plaintiffs and the Class.

98. Defendant had full knowledge of the sensitivity of the Confidential Information and the types of harm that Plaintiffs and the Class could and would suffer if the Confidential Information were wrongfully disclosed.

99. Defendant had a duty to Plaintiffs and each Class member to exercise reasonable care in holding, safeguarding, and protecting that information.

100. Plaintiffs and the Class Members were the foreseeable victims of any inadequate safety and security practices.

101. Plaintiffs and the Class Members had no ability to protect their Confidential Information that was in TQL's possession.

102. Defendant was well aware of the fact that cyber criminals routinely target large companies through software vulnerabilities and phishing attacks and other cyberattacks in an attempt to steal Confidential Information.

103. Defendant knew or should have known that failing to segmented its IT systems or encrypt Confidential Information greatly increased the likelihood of a data breach and increased the potential harm that such a data breach would cause.

104. Defendant owed Plaintiffs and the Class member a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiffs and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data.

105. Defendant's duty extended to protecting Plaintiffs and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B; *see also Simpson v. Big Bear Stores Co.*, 652 N.E.2d 702, 705 (Ohio 1995).

106. Defendant knew or should have known the risk of collecting and storing the Confidential Information and the importance of maintaining secure systems.

107. Defendant had duties to protect and safeguard their Confidential Information from unauthorized disclosure. Defendant had a duty to use reasonable, industry standard information security measures when dealing with sensitive Confidential Information. Specific duties that TQL owed Plaintiffs and the Class include:

a. To create, maintain, and comply with a written cybersecurity program that incorporated physical, technical, and administrative safeguards for the protection of personal information and reasonably conforms to an industry recognized cybersecurity framework;

b. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting the Confidential Information in its possession;

c. To protect the Confidential Information in its possession using reasonable and adequate security procedures and systems, including firewalls and encryption;

d. To adequately and properly audit, scan, monitor, and test its IT systems for vulnerabilities and intrusions;

e. To adequately and properly audit, test, and train its employees regarding how to properly and securely transmit and store Confidential Information;

f. To implement processes to quickly detect a data breach, security incident, or intrusion;

g. To adequately audit and oversee the information security of any third-parties it contracted with, including mobile app developers; and

h. To promptly notify Plaintiffs and Class Members of any data breach, security incident, or intrusion that affected or may have affected their Confidential Information.

108. Defendant owed these duties to Plaintiffs and the Class because they are a well-defined, foreseeable, and probable class of persons whom Defendant was aware (or should have been) would be injured by Defendant's breach of these duties.

109. Plaintiffs and the Class were the intended beneficiaries of Defendant's duties, creating a special relationship between them and TQL. Defendant was in a position to ensure that its systems were sufficient to protect the Confidential Information that Plaintiffs and the Class had entrusted to it.

110. Defendant breached its duties of care by failing to adequately protect Plaintiffs' and the Class's Confidential Information. Defendant breached its duties by, among other things:

a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the Confidential Information in its possession;

b. Failing to protect the Confidential Information in its possession using reasonable and adequate security procedures and systems;

c. Failing to adequately and properly audit, scan, monitor, and test its IT systems to identify and correct vulnerabilities;

d. Failing to implement and enforce adequate security policies, systems, protocols and practices sufficient to protect the Confidential Information, and thereby creating a foreseeable, unreasonable risk of harm;

e. Failing to adequately and properly audit, test, and train its employees regarding how to properly and securely protect Confidential Information;

f. Failing to comply with the minimum industry data security standards, including the guidelines issued by the FTC, to protect the Confidential Information it solicited and retained;

g. Failing to consistently enforce security policies aimed at protecting Plaintiff and the Class's Confidential Information; and

h. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions.

111. Defendant's willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

112. As a proximate and foreseeable result of Defendant's grossly negligent conduct, Plaintiffs and the Class have suffered actual damages, as described above, and are at imminent risk of additional harms and damages.

113. The damages Plaintiffs and the Class have suffered were and are reasonably foreseeable.

114. The damages Plaintiffs and the Class have and will suffer were and are the direct and proximate result of Defendant's grossly negligent conduct.

115. Plaintiffs and the Class have suffered injury and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
BREACH OF CONTRACT
(On Behalf of the Class, or alternatively the Carrier Subclass)

116. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

117. Plaintiffs and all other motor carriers entered into broker-carrier agreements with TQL that contained a substantially similar confidentiality agreement requiring TQL to protect the Confidential Information of Plaintiffs and the Class.

118. Plaintiff Finesse entered into its agreement with TQL on June 5, 2019, a true and accurate copy of which is attached as **Exhibit B**.

119. The confidentiality agreement contained in Plaintiff Finesse's agreement with TQL is substantially the same as that contained in Plaintiff Wider's and all other Class members who are carriers' agreements with TQL.

120. The confidentiality agreement provides the following:

> **CONFIDENTIALITY**. In addition to confidential information protected by law, whether statutory or otherwise, the Parties agree that all of their financial information and that of CUSTOMERS, including, without limitation, freight and brokerage rates, amounts received for brokerage services, amounts of freight charges collected, amounts of freight charges paid, freight volume requirements, as well as related CUSTOMER information, CUSTOMER shipping or other logistic requirements shared or learned between the Parties and CUSTOMERS shall be treated as confidential, and shall not be disclosed or used for any reason without prior written consent by the Parties. If confidentiality is breached, the Parties agree that the remedy at law, including monetary damages, may be inadequate and that the Parties shall be entitled, in addition to any other remedy available, to an injunction restraining the violating Party from further violation of this Agreement.

See, e.g., **Exhibit B** (Broker-Carrier Agreement between TQL and Finesse Express, LLC, executed June 5, 2019, ¶ 21).

121. The Confidential Information exposed in the Data Breach falls within the protection of this provision.

122. TQL violated this provision by not treating the Confidential Information as confidential through its failure to implement the necessary data security policies, rules, and procedures to protect the Confidential Information from hackers.

123. Plaintiffs have and will continue to suffer monetary losses as a result of TQL's violation of this provision, including foreseeable consequential damages that Defendant knew about when it entered into the confidentiality agreement and requested Plaintiffs' and the Class Members' Confidential Information.

124. As the parties agreed, monetary damages alone are inadequate to fully remedy TQL's breach of this confidentiality agreement. Thus, Plaintiffs and the Class are entitled to an injunction in addition to monetary damages.

125. Accordingly, Plaintiffs and the Class are entitled to compensatory damages in an amount to be determined by a jury, to injunctive relief requiring TQL to maintain the confidentiality of the Confidential Information of Plaintiffs and the Class, and to the attorney fees, costs, and expenses incurred in bringing this action.

THIRD CAUSE OF ACTION
UNJUST ENRICHMENT
(On Behalf of the Class)

126. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

127. Plaintiffs and the Class bring this claim in the alternative to all other claims and remedies at law.

128. Defendant, by way of its affirmative actions and omissions, including its knowing violations of its contracts with Plaintiffs and the Class and common law duties of care, knowingly and deliberately enriched itself by saving the costs it reasonably and contractually should have expended on data security measures to secure Plaintiffs' and Class Members' Confidential Information.

129. Instead of providing for a reasonable level of security that would have prevented the Data Breach, as described above and is common industry practice among companies entrusted with similar Confidential Information, Defendant instead consciously and

opportunistically calculated to increase its own profits at the expense of Plaintiffs and Class Members.

130. While it cut costs on security, Defendant continued to obtain the benefits conferred on it by Plaintiffs' and the Class, including brokerage fees premised in part upon the confidentiality agreement and other representations that it would adequately protect the Confidential Information.

131. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security and the resulting disclosure of the Confidential Information, Plaintiffs and Class Members suffered and continue to suffer considerable injuries.

132. Defendant therefore engaged in an opportunistic behavior and was unjustly enriched when it profited from Plaintiffs and the Class by promising to protect their Confidential Information but failing to invest the necessary resources into doing so. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its breach.

133. Accordingly, Plaintiffs on behalf of themselves and the Class, are entitled to relief in the form of restitution and/or compensatory damages.

FOURTH CAUSE OF ACTION
INJUNCTIVE AND DECLARATORY RELIEF
(On Behalf of the Class)

134. Plaintiffs incorporate by reference all preceding factual allegations as though fully alleged here.

135. Plaintiffs and the Class bring this claim in addition to all other claims and remedies.

136. This count is brought under the Federal Declaratory Judgment Act, 28 U.S.C. § 2201.

137. As previously alleged and pleaded, Defendant owes duties of care to Plaintiffs and the Class that require it to adequately secure their Confidential Information.

138. Defendant still possesses the Confidential Information of Plaintiffs and the Class.

139. Defendant has not satisfied its contractual obligations and legal duties to Plaintiffs and the Class.

140. Defendant has claimed that it is taking some steps to increase its data security, but there is nothing to prevent Defendant from reversing these changes once it has weathered the increased public attention resulting from this Breach, and to once again place profits above data protection.

141. Plaintiffs, therefore, seek a declaration (1) that Defendant's existing security measures do not comply with its contractual obligations and duties of care to provide adequate security, and (2) that to comply with its contractual obligations and duties of care, Defendant must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering Defendant to engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering Defendant to engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Defendant audit, test, and train their security personnel regarding any new or modified procedures;

d. Ordering that Defendant segment carrier and customer data by, among other things, creating firewalls and access controls so that if one area of Defendant's systems is compromised, hackers cannot gain access to other portions of Defendant's systems;

e. Ordering that Defendant implement encryption rules on all IT systems containing Confidential Information of carriers and customers;

f. Ordering that Defendant purge, delete, and destroy in a reasonably secure manner Confidential Information not necessary for its provisions of services;

g. Ordering that Defendant conduct regular database scanning, vulnerability, and securing checks;

h. Ordering Defendant to routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

i. Ordering Defendant to implement and enforce adequate retention policies for Confidential Information, including destroying carrier and customer Confidential Information as soon as it is no longer necessary for the purposes it was originally acquired; and

j. Ordering Defendant to meaningfully educate its current, former, and prospective employees and subcontractors about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps they must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs Finesse Group, and the Class pray for judgment against Defendant as follows:

a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Class requested herein;

b. A judgment in favor of Plaintiffs and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;

c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. An order requiring Defendant to pay the costs involved in notifying the Class about the judgment and administering the claims process;

e. A judgment in favor of Plaintiffs and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and

f. An award of such other and further relief as this Court may deem just and proper.

Respectfully submitted,

/s/ Marc E. Dann, Esq.
Marc E. Dann (0039425)
Brian D Flick (0081605)
DANNLAW
P.O. Box 6031040
Cleveland, OH 44103
Phone: (216) 373-0539
Facsimile: (216) 373-0536
notices@dannlaw.com

William B. Federman
(S.D. New York #WF9124)
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Ave.
Oklahoma City, Oklahoma 73120
(405) 235-1560
(405) 239-2112 (facsimile)
wbf@federmanlaw.com
Pro Hac Vice Application to be submitted

Cornelius P. Dukelow
Abington Cole + Ellery
320 South Boston Avenue, Suite 1130
Tulsa, OK 74103
Telephone and Facsimile: (918) 588-3400
cdukelow@abingtonlaw.com
Pro Hac Vice Application to be submitted

Counsel for Plaintiffs Finesse Express, LLC and Wider Group, Inc. and the Putative Class

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all appropriate issues raised in this Complaint.

/s/Marc E. Dann, Esq.
Marc E. Dann, Esq.
Counsel for the Plaintiffs and the Putative Class